METHOD AND APPARATUS FOR SECURING FACILITIES AGAINST UNAUTHORIZED ACCESS, IN PARTICULAR FOR IDENTIFYING GAMBLERS IN A CASINO

[0001] The invention relates to a method and an apparatus for securing facilities against access of unauthorized persons, in particular for verifying the access authorization of gamblers to gambling machines in a casino, wherein biometric data of the persons are analyzed.

[0002] In manifold applications, security systems are used to refuse access to certain areas or facilities to unauthorized persons. Such areas are, for example, gambling machines in casinos, cash machines, laboratory premises to be kept secret and the like. Thereby, it is also known to use facilities for acquiring biometric data.

[0003] Here, an important measure is to prevent the misuse of data media provided with cash value.

[0004] For this, according to DE 198 42 355, a method for encashing an amount for the authorized use of an area and/or a service is known, where the unauthorized use of a data medium is prevented by storing data in a data terminal at the beginning of use and calculating the amount payable for the period of use after the termination of use, wherein a value transponder containing an individual identification number and a certain debitable amount is linked to a read/write station of the data terminal and a deposit amount on the value transponder is blocked at the beginning of use and the amount calculated for the period of use is debited and the blocking of the deposit amount is canceled after termination of use. This way it can be achieved that no reverse postings onto the transponder, but only a release of blockings at simultaneous fee debits are carried out at the voucher machine. Thus, manipulations in order to unjustifiedly withdraw money are impossible.

[0005] Here, it is disadvantageous that the user has to connect to the data terminal several times and that he is not protected against loss of the value transponder nor its unauthorized use.

[0006] In WO 02/47042, a system to operate gambling machines in a casino is described, where biometric data of users are stored in a computer and the access authorization of the gamblers is verified using these data.

[0007] In this case, it is disadvantageous that this system is not suitable for a larger number of users, because the very large amounts of data to be verified require a too large expenditure of time.

[0008] The invention is underlied by the problem to specify a method and an apparatus of the kind initially mentioned, by which a high security is assured for the unauthorized use of facilities. The invention shall enable a cost-effective and fast verification and avoid to a large extent verification processes that burden the user.

[0009] According to the invention, the problem is solved by a method comprising the attributes given in claim 1.

[0010] Advantageous embodiments are given in the dependent claims.

[0011] The method according to the invention enables to carry out a preselection of data from a large database very fast and cost-effective. For example, the data of 50 000 gamblers can be stored in a central database and from there, a gambling machine gathers the datasets of the gamblers located in its vicinity which will be a very much smaller quantity, so even in the case of a number of 500 gamblers these data can be analyzed within less than one second without problems.

[0012] In the following, the invention is further explained considering an embodiment as an example. The example describes the process in a casino with a plurality of gamblers and gambling machines.

[0013] In the appropriate drawings, it is shown by:

[0014] Figure 1 the process of registering a gambler,

[0015] Figure 2 the finger identification and the assignment of the gamblers to the gambling machines located within reach,

[0016] Figure 3 the start of a game by touchless finger identification and

[0017] Figure 4 a schematic representation of an arrangement for touchlessly acquiring a finger by means of two detectors.

[0018] In Figure 1, two persons P are depicted who possess as a document D, respectively, a gambler identity card on which a photograph and a fingerprint of the persons P are mounted and which is provided with a radio chip. If the person P approaches the facility E, i. e. in the case under consideration the gambling machine, the biometric data of the gambler are loaded by the gambling machine as soon as the range of its radio chip being mounted on the document D detects the gambling machine. If the person P departs from the radio range these data are deleted automatically. The gambling machine thus has the relevant data of all persons P being located within the radio range at its disposal.

[0019] In Figure 2, there is illustrated the finger identification and the assignment of the biometric data of all gamblers located within reach to the gambling machines arranged there.

[0020] The start of a game shown in Figure 3 is performed by means of the key S which becomes operative by touchless identification of a finger of a person P.

[0021] Figure 4 explains the basic way of operation of a facility for fraud-proof verification by simultaneously acquiring two partial images of the finger 1 from different directions. The position of the finger is defined by the coordinates x, y, z in a Cartesian coordinate system. As shown in this illustration, this finger is simultaneously acquired from a different angle of view in addition to the detector 2.1 which is located in the x-y plane and acquires the image of the finger 1 in z-direction, wherein this image results from laying onto a sensor or, preferably, from

imaging. Preferably, the directions of imaging, from which the object is observed, form an angle of 90 degrees and lie in one plane. This means, that the angles φ and δ between the direction of taking and a coordinate direction running through the finger's axis as y-axis, which are depicted in Figure 1, have a value of 90°. A second image is taken in x-direction by the detector 2.2 which is located in the y-z plane.

[0022] The function values are compared to data of reference functions which exhibit an identical data structure and are stored in a data base.

[0023] The reference functions, then, look like

$R_{xy}(x, y, m_{xy})$ for the reference image in the x-y plane, with which the image F_{xy} taken in the x-y plane by the detector 2.1 has to be concordant

and

$R_{yz}(z, y, m_{yz})$ for the reference image in the y-z plane, with which the image taken in the y-z plane by the detector 2.2 has to be concordant.

[0024] The object is recognized to be right if a satisfying amount of data, e. g. 90%, are concordant for F_{xy} and R_{xy} as well as for F_{yz} and R_{yz}, respectively. The images of the dermal ridges can be described by recognition functions of the form F(x, y, z, m).

[0025] For the arrangement depicted in Figure 1, the function

$F_{xy}(x, y, m_{xy})$

describes the image taken by the detector 2.1 in the x-y plane

and the function

$F_{yz}(z, y, m_{yz})$

describes the image taken by the detector 2.2 in the y-z plane,

wherein m_{xy} and m_{yz} describe characteristic recognition attributes of dermal points in the respective planes.

[0026] List of reference numbers

P	Person
D	Document
S	Key
E	Facility
1	Finger
2	Light detector
3	Light source
3.1 ... 3.4	Light sources positioned adjacently to a light detector